RYAN TYZ (CSB No. 234895)
ryan@tyzlaw.com
ERIN JONES (CSB No. 252947)
ejones@tyzlaw.com
DEBORAH HEDLEY (CSB No. 276826)
deborah@tyzlaw.com
STEPHANIE ALVAREZ SALGADO (CSB No. 334886)
stephanie@tyzlaw.com
TYZ LAW GROUP PC
4 Embarcadero Center, 14th Floor
San Francisco, CA 94111
Telephone: 415.868.6900

Attorneys for Defendant
Fandom, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

VISHAL SHAH and JAYDEN KIM, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FANDOM, INC.,

Defendant.

Case No: 3:24-cv-01062-RFL

DEFENDANT FANDOM, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

Date: September 10, 2024
Time: 10:00 a.m.
Courtroom: 15, 18th Floor

FAC Filed: April 29, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

RULES

NOTICE OF MOTION AND MOTION

TO THE COURT AND PLAINTIFFS AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on September 10, 2024 at 10:00 a.m. or as soon thereafter as counsel may be heard in the courtroom of the Honorable Rita F. Lin, Courtroom 15, 18th Floor of the United States District Courthouse located at 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant, Fandom, Inc. ("Fandom") will and hereby does move the Court for an order dismissing the First Amended Complaint of Plaintiffs Vishal Shah and Jayden Kim pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. This Motion is based on the Notice of Motion and Motion, the Memorandum of Points and Authorities and the Request for Judicial Notice it contains, the Declaration of Erin Jones and its attached exhibits, the Court's files in this action, the arguments of counsel, and any other matter that the Court may properly consider.

Fandom respectfully requests that the Court (1) grant its request for judicial notice, and (2) issue an order dismissing the Complaint with prejudice under Federal Rule of Civil Procedure 12(b)(6) for failure to state any claim upon which relief may be granted.

ISSUES TO BE DECIDED

1. Whether Plaintiffs have failed to state a claim under Section 638.51(a) of the California Invasion of Privacy Act where they voluntarily provided their information to Fandom and have not plausibly alleged installation or use of a pen register under CIPA.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs Vishal Shah and Jayden Kim ("Plaintiffs") voluntarily provided their IP addresses to Fandom every one of the "multiple times" that they used web browsers on their desktop computers to visit Fandom's Gamespot.com website. Indeed, Plaintiffs' computers necessarily had to provide their IP addresses to Fandom so that Fandom's web server could respond to their requests and send back instructions and data to Plaintiffs' web browsers, so they could display the Gamespot.com website. Despite these facts, Plaintiffs bring this putative class action, claiming that software that collected their IP addresses when they visited Fandom's website was an illegal "pen register" under Section 638.51 of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 et seq. They seek $5,000 in statutory damages for each alleged violation.

Plaintiffs' claim has no merit. State and federal court decisions have made clear that the collection of a user's IP address by a website operator cannot support a pen register claim because users voluntarily and necessarily provide that IP address to the website operator to access its webpages. The claim also runs contrary to both the intent of the legislature in enacting the pen register law and its plain language, which make clear that a pen register is a device or process that records "dialing, routing, addressing, or signaling information" of an outgoing communication, not the user's own number. Plaintiffs' contrary interpretation of the law would convert fundamental and essential internet operations into criminal acts subject to damages under CIPA. This cannot be an intended consequence of CIPA. The Court should reject Plaintiffs' attempt to expand California's criminal pen register statute beyond its text and purpose.

This case is part of a recent wave of nearly identical lawsuits filed by Plaintiffs' counsel across the country. Using similar language and figures, the complaints allege that a website operator's collection and sharing of a user's IP address involves an illegal "pen register" that violates Section 638.51. At current count, at least ten cases have been filed, including against the Los Angeles Times, CNN, and Buzzfeed, all alleging a similar claim under Section 638.51 involving third-party code. *See* Declaration of Erin Jones ("Jones Decl."), Exs. 1-9 (listing

cases).[1] As here, most of the cases target website operators like Fandom, rather than the third parties that Plaintiffs allege developed and used the software that allegedly collected their IP addresses. This also highlights a disconnect between this case and the purposes of CIPA.

Accordingly, Plaintiffs' sole cause of action under Section 638.51 fails to state a claim under Federal Rule of Civil Procedure 12(b)(6). First, collection of a user's IP address by a website operator to whom it was voluntarily and necessarily provided cannot support a Section 638.51 claim. Second, Plaintiffs' allegations show that the code Plaintiffs accuse of collecting their IP addresses (the "Accused Code") fails to meet CIPA's definition of a "pen register," both because it does not collect addressing information for the outgoing communications, and to the extent Plaintiffs complain the Accused Code collected the content of communications (as the pen register definition excludes devices that collect such content). Third, the Accused Code does not fall under CIPA because it does not involve telephone surveillance and tracking. Fourth, Plaintiffs fail to plausibly allege that Fandom used or installed the Accused Code.

Plaintiffs' claims are defective at their core and no facts can save them. Therefore, Fandom respectfully requests dismissal with prejudice.

II. PROCEDURAL HISTORY

Plaintiff Vishal Shah filed his initial complaint in the San Francisco Superior Court on January 8, 2024. *See* Dkt. 1-1. Fandom removed the case to this court under the Class Action Fairness Act, Dkt. 1, and Plaintiff Shah did not seek to remand. When Fandom moved to dismiss Plaintiff Shah's initial complaint for failure to state a claim under Rule 12(b)(6), Dkt. 11, he chose to amend rather than oppose the motion. *See* Dkt. 13. But although the first amended complaint ("FAC") added a new plaintiff, some additional background information, and a few tweaks to the allegations, *see* Dkt. 15-1, it did not add facts addressing the deficiencies detailed in Fandom's first motion to dismiss. Fandom now moves to dismiss the FAC with prejudice.

[1] The Court can take judicial notice of such court filings on a motion to dismiss. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1024-25 (N.D. Cal. 2014) (taking judicial notice). On this basis, Fandom requests the Court take judicial notice of Exhibits 1-10 and 14 of the Jones Declaration.

III. RELEVANT FACTS

A. Fandom's Gamespot.com Website

Fandom's website Gamespot.com (the "Website") is a popular, publicly accessible gaming website that "provides news, reviews, previews, downloads, and other information about video games" over the internet. Dkt. 15, ¶ 62.

To access Gamespot.com (or any website on the internet), a user must have and disclose an IP address associated with his or her computer (*i.e.*, the user's "source" IP address) to Gamespot.com. Providing the user's source "IP address enables a device to communicate with another device—such as a computer's browser communicating with a server." *See id*. ¶ 25. Specifically, "[t]o make Defendant's Website load on a user's internet browser, the browser sends an 'HTTP request' or 'GET' request to" Fandom's web server. *Id.*, ¶ 21, Figure 1. Such a "user request for a page or file" necessarily "includes the IP address of the user's computer, and the name of the requested page or file, among other things." *See Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *2 (C.D. Cal. May 29, 2007); *United States v. Christie*, 624 F.3d 558, 563 (3d Cir. 2010) ("IP addresses are . . . conveyed to websites that an internet user visits"). When Fandom's web server receives the user request, it uses the source IP address provided in the user request to send an HTTP response, containing instructions to the user's browser for how to display Gamespot.com, including "what images to load, what text should appear, or what music should play." *See* Dkt. 15, ¶¶ 22, 21, Figure 2; *see also Columbia*, 2007 WL 2080419, at *2 ("The web server interprets and processes that data… in order to respond to user requests.") A web server can generally access and record users' source IP addresses when it services their webpage requests. *See id*. at *11 ("IP addresses" are "necessarily capture[d] … to operate the website."); *Christie*, 624 F.3d at 563 ("administrators of websites . . . can see the IP addresses of visitors to their sites."). Because IP addresses are generally assigned to users by the company that provides them with internet access, the IP address can indicate the "state, city, and zip code" where the device is located. *See* Dkt. 15, ¶ 26.

B. The Accused Code

Plaintiffs allege that Fandom's server also "causes" a user's browser to install three pieces

of software code from third parties GumGum, Audiencerate, and TripleLift (collectively, the "Accused Code"), which allegedly record users' source IP addresses. *Id.*, ¶ 23 (Plaintiffs refer to the Accused Code as "trackers"). According to the FAC, the Accused Code can instruct a user's browser to send the user's IP address to GumGum, Audiencerate and TripleLift in one of two ways: (1) "as standalone data" after a user visits the Website for the first time, or (2) in subsequent visits to the website, "through [a] cookie" installed by the Accused Code. *Id.*, ¶¶ 37, 38, 47, 48, 73. Plaintiffs allege that the third-party "operators of the [Accused Code] then use the IP address of Website visitors" for advertising and to "conduct website analytics." *Id.* ¶ 69. Plaintiffs do not allege that any user information, including the user's IP address, is communicated to Fandom's server through the Accused Code. *See, e.g.*, *id.* Figures 4, 5 (showing information sent to GumGum and Audiencerate, not Fandom, allegedly containing IP address information).

C. Plaintiffs

Plaintiffs Vishal Shah ("Shah") and Jayden Kim ("Kim") claim to have visited Fandom's Gamespot.com website "multiple times" using browsers on their "desktop" computers. *Id.*, ¶ 89 (Shah), ¶ 96 (Kim). Plaintiffs allege that on visiting the website, Fandom "caused" the Accused Code to be installed on their web browsers. *Id.* ¶¶ 90, 97.

Plaintiff Shah alleges that the Accused Code collected and sent his IP address to GumGum and Audiencerate within cookies. *Id.* ¶ 91 (IP address sent "via the GumGum cookie" and "within the cookie"); ¶ 90 (claiming Figure 11 shows collection of IP address by Audiencerate tracker); Figure 11 (showing IP address contained within the text of the "Cookie"); *see also* Figure 10 (same). Plaintiff Shah also speculates that on his first visit to Gamespot.com, his IP address would have been sent as "standalone data" rather than through a cookie. *Id.* ¶ 91. Plaintiff Kim alleges that "TripleLift … used the TripleLift [code] to collect Plaintiff Kim's IP address" but does not specify how the IP address was sent to TripleLift. *Id.*, ¶ 97 (citing Figure 6); Figure 6 (identifying with a red box an IP address inside the body of a cookie transmission); *see also id.* ¶¶ 57, 58. Although Plaintiffs claim generally that "Defendant [Fandom] … used the [Accused Code] to collect Plaintiffs' and Class Members' IP addresses," *id.* ¶¶ 118, 90, 97, as above, they do not claim that the Accused Code communicates any information to Fandom.

Based on these facts, Plaintiffs bring a single claim, arguing that Fandom violated Cal. Penal Code Section 638.51 by causing the installation of the Accused Code – which Plaintiffs argue is a "pen register"– and by using that code to collect the IP addresses of Plaintiffs' desktop computers. Plaintiffs do not contend that the Accused Code is a "trap and trace" device. *See, e.g.,* Dkt. 15 ¶¶ 115-117.

IV. LEGAL STANDARDS

To survive against a motion to dismiss, a complaint must state factual allegations sufficient "to raise a right to relief above the speculative level" and provide "enough facts to state a claim to relief that is plausible on its face." *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("[T]he pleading standard Rule 8 announces . . . demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation.") A claim is plausible only if the plaintiff alleges enough facts to support a reasonable inference that the defendant is liable for the alleged misconduct. *Iqbal*, 556 U.S. at 678 . "A pleading that offers 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555).

On a motion to dismiss, "courts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

Here, Plaintiffs' FAC does not cross the threshold from possibility to plausibility and must be dismissed with prejudice.

V. PLAINTIFFS CANNOT STATE A PLAUSIBLE CLAIM UNDER SECTION 638.51(a) OF THE CALIFORNIA INVASION OF PRIVACY ACT (CIPA)

Plaintiffs' single claim under Section 638.51(a) fails to show a plausible right to relief.

A. Code that Records Users' Voluntarily Provided Source IP Addresses Does Not Violate Section 638.51

The Court should dismiss Plaintiffs' sole cause of action because Section 638.51(a) does not apply to Fandom's collection of a user's IP address, which the user necessarily and voluntarily discloses to Fandom to visit the website. *See Licea v. Hickory Farms, LLC*, Case No.

23STCV26148, Minute Order at 6 (Cal. Super. Ct. L.A. Cnty. March 13, 2024) (sustaining demurrer to Section 638.51 claim) (provided as Jones Decl., Ex. 14); *see Columbia,* 2007 WL 2080419, at *2 (a "user request for a page or file" necessarily "includes the IP address of the user's computer"); *Christie*, 624 F.3d at 563 ("IP addresses are . . . conveyed to websites that an internet user visits"); *U.S. v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008) (IP addresses "are voluntarily turned over in order to direct . . . third party[] server[s]" and so no reasonable expectation of privacy attaches to them). Accordingly, both California and federal courts have refused to apply pen register law to IP address collection, as described below. The Court should reject Plaintiffs' invitation to deviate from this history and expand California pen register law in a direction that risks criminalizing the fundamental operation of the internet.

Although the recent wave of cases seeking to apply pen register law to this basic internet functionality is only nascent, early decisions have already rejected Plaintiffs' theory here. The Los Angeles Superior Courts recently dismissed two Section 638.51 cases asserting that technology used to collect IP addresses on a website was a pen register. *See Licea*, Minute Order at 1, 6; *Casillas v. Transitional Optical, Inc*., Case No. 233STCV30742, Minute Order at 1, 4 (Cal. Super. Ct. L.A. Cnty. April 23, 2024) (provided as Jones Decl., Ex. 10) (dismissing pen register claim alleging "that Defendant's website … deployed tracking software that relies upon the user's unique Internet Protocol address (IP address)"). Citing federal cases, *Licea* dismissed a pen register claim against a website operator "where an IP address may be voluntarily disclosed" to that operator by users whenever they visit its site. *Licea,* Minute Order at 6 (citing *Forrester*, 512 F.3d at 510 (federal pen register case)). The court particularly recognized that the user's necessary and voluntary provision of his IP address to the website "under the guise of visiting" the site raised an issue of "consent" negating the CIPA pen register claim. *Id*. at 6; *compare* Section 638.51(b) (providing that the provider of an electronic communication service may use a pen register "[i]f the consent of the user of that service has been obtained."). In summary, the court emphasized that the impact on the internet would be extreme if plaintiff's interpretation prevailed and the collection of user IP addresses by website operators were criminalized, explaining: "public policy strongly disputes Plaintiff's potential interpretation of privacy laws as

one rendering every single entity voluntarily visited by a potential plaintiff, thereby providing an IP address for purposes of connecting the website, as a violator." *Id*.

These California decisions harmonize with the federal courts' longstanding refusal to apply federal pen register laws (18 U.S.C. § 3121 et seq.) to the collection of IP addresses by a website operator. This makes sense because the California pen register laws were patterned after the federal laws and mirror them in relevant aspects. *See* Jones Decl., Ex. 12 (June 16, 2015 Hearing on AB 929)[2] (reciting multiple provisions from 18 U.S.C. §§ 3121 et seq. in describing the "PURPOSE" of AB 929 that enacted California provisions); *also compare* Cal. Penal Code § 638.51(a) ("a person may not install or use a pen register or a trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53") with 18 U.S.C. § 3121(a) ("no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title"); Cal. Penal Code § 638.50(b) ("Pen register" means a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.") with 18 U.S.C. § 3127(3) (almost identical).

Applying these analogous laws, federal courts have found that an "IP address is transmitted as part of the normal process of connecting one computer to another over the Internet" and consequently that "the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then *the Internet could not function* because standard computer operations require recording IP addresses so parties can communicate with one another over the Internet." *Capitol Recs. Inc. v. Thomas-Rasset*, No. CIV 06-1497(MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. June 11,

[2] The Court can take judicial notice of the legislative history of California Assembly Bill 929, which enacted the CIPA pen register provisions asserted by Plaintiffs. *See In re Yahoo*, 7 F. Supp. 3d at 1024 (taking judicial notice of legislative history and granting in part motion to dismiss). On this basis, Fandom requests the Court take judicial notice of Exhibits 11-13 to the Jones Declaration.

2009) (emphasis added). Applying this understanding, the court in *Capitol Records* rejected an argument that collection of IP addresses, including "the IP address of the source of the packet," during peer-to-peer file sharing violated the federal pen register act. *Id*. at *1, *3. Likewise, in *Malibu Media, LLC v. Pontello,* the court rejected an allegation that Malibu's "tracking the IP addresses" of users that shared its videos on the BitTorrent network constituted an unlawful pen register. *Malibu*, No. 13-12197, 2013 WL 12180709, at *3, *4 (E.D. Mich. Nov. 19, 2013) (rejecting unclean hands defense based on pen register allegation). The court found that this IP address collection was not prohibited by the federal pen register law: "By participating in … BitTorrent," the court found that users had "consensually engaged" and "communicated his IP address as part of the packet his computer sent to [Malibu's investigator]. Because the IP address was voluntarily sent, the Pen Register Act cannot prevent Malibu's investigator from recording that information." *Id*. at *4.

Likewise, here, the Court should decline to apply pen register law to the Accused Code on Fandom's website. Like the cases above, Plaintiffs' pen register claim is based entirely on Fandom's alleged collection of the source IP addresses that Plaintiffs voluntarily provided to Fandom's website "multiple times" in order to display and view the website on their browsers. *See* Dkt. 15, ¶ 89, 96; *Columbia*, 2007 WL 2080419, at *2 (a "user request for a page or file" necessarily "includes the IP address of the user's computer, and the name of the requested page or file, among other things"); *Christie*, 624 F.3d at 563 ("IP addresses are . . . conveyed to websites that an internet user visits"). And no different from using "tracking software" (*Casillas*), "packet capture technology" (*Capitol Records*) or an investigator (*Malibu Media),* use of third-party Accused Code to capture data already provided to Fandom's servers by Plaintiffs' actions in accessing Fandom's website does not violate the California penal code. *Casillas,* Minute Order at 3-4; *Capitol Records*, 2009 WL 1664468, at *1; *Malibu*, 2013 WL 12180709, at *4; *see also Licea*, 2024 WL 1698147, at *1, 6. The mere communication and disclosure of Plaintiffs' IP addresses, which "public websites" like Fandom's receive from "all visiting users" by nature of how the internet works—is not an unlawful use of a "pen register" under CIPA. *See United States*

v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *1 (C.D. Cal. Aug. 8, 2016), *aff'd*, 800 F. App'x 571 (9th Cir. 2020).

Plaintiffs may attempt to argue otherwise by comparing their facts to the out-of-district case cited in their complaint, *Greenley v. Kochava*, *Inc*., No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023). But the facts of *Greenley* are very different and do not apply here. For example, the *Greenley* plaintiff alleged that he was unaware of and had not consented to the collection of a large volume and variety of highly personal data (including "'personal information,' geolocation data, and communications from his cellular telephone") by the software at issue in that case. *Id*. at **1, **3. Whereas here, Plaintiffs allege only the collection of a single piece of information that was already necessarily communicated to Fandom (and to every other website they visit) through fundamental internet operations. In addition, *Greenley* involved parties with a very different relationship. The *Greenley* defendant was the third-party data broker that had provided tracking software to application operators and then surreptitiously mined volumes of sensitive user data from it, *id*. **1, but here, Fandom is the operator of the website, not the provider or operator of the Accused Code. For analogous reasons and others, other courts have declined to follow *Greenley* and declined to apply Section 638.51 to website operators' collection of IP addresses. *See Casillas*, Minute Order at 3 (distinguishing *Greenley* on the basis of the "very different" "alleged conduct and relationship to the plaintiff").

As demonstrated above, the weight of California and federal pen register cases confirm that Section 638.51 does not apply here "[b]ecause [Plaintiff's] IP address was voluntarily sent" to Fandom's website. *See Malibu Media*, 2013 WL 12180709, at *4. The Court should dismiss Plaintiffs' FAC accordingly.

B. The Accused Code is Not a Pen Register

The Court should dismiss Plaintiffs' claim under Cal. Penal Code § 638.51 because the Accused Code is not a "pen register." No court has ever found such code—which Plaintiffs acknowledge collects nothing more than the IP addresses of their home desktop computers—to be a pen register. Under CIPA, a "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument … from which

a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b). A "pen register" "does not include a device or process used by a provider … of a wire or electronic communication service" for provision of services, billing purposes, cost accounting, "or other similar purposes in the ordinary course of its business." *Id*. In addition, "[a] provider of electronic or wire communication service may use a pen register" to operate, maintain and test its service, protect the rights and property of the provider, protect the users of the service, or with the "consent of the user." § 638.51(b). Because the Accused Code does not fit within the plain text of the pen register definition, and Fandom's circumstances invoke many of its exceptions, Plaintiffs' claims fail.

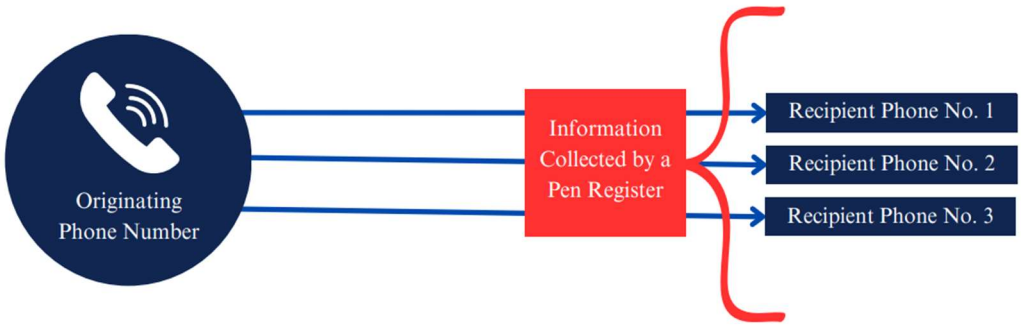
i. The Accused Code Does Not Capture Addressing Information of an Outbound Communication

The Accused Code is not a "pen register" because it does not perform the basic function of a pen register: capturing the "dialing, routing, addressing, or signaling information" associated with a "communication" "transmitted by an instrument." § 638.50(b). Traditionally, a pen register was a mechanical device installed on a landline telephone to measure its outgoing electrical impulses, thereby revealing the phone number being dialed—*i.e.*, the *recipient* address of the outbound communication. *See Smith v. Maryland,* 442 U.S. 735, 736 n. 1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."); *People v. Larkin*, 194 Cal. App. 3d 650, 653 n.2 (1987) ("A pen register is a mechanical device connected to a telephone number to monitor dialing activity. It registers the phone numbers dialed to make outgoing calls, including the dates and times the receiver is picked up and replaced."). Accordingly, a pen register enables law enforcement officers to identify the persons to whom targeted individuals in a criminal investigation are speaking. *See, e.g., United States v. Jadlowe*, 628 F.3d 1, 5–6 (1st Cir. 2010) ("Law enforcement agents concluded that 'Uncle Marc' was Jadlowe based on, inter alia, pen register data obtained from Gonsalves's phone showing that Gonsalves frequently exchanged calls with a phone number the agents linked to Jadlowe.").

Section 638.50 (which defines "pen register" as used in Section 638.51) reflects this same

fundamental purpose of a pen register—to capture the "dialing, routing, addressing, or signaling information" transmitted by a device in connection with a communication being sent— that is, the *recipient* information of the outbound communication. The legislative history for California Assembly Bill 929, which enacted California's pen register provisions (Section 638.50 et seq.), confirms that this was Section 638.50's purpose: to provide law enforcement with a tool "to record all outgoing numbers from a particular telephone line." *See* Jones Decl., Ex. 12 at 10 (June 16, 2015 Hearing on AB 929). The California statute includes both "devices" and "processes," such as software, that provide the pen register function. § 638.50(b). The operation of a pen register according to these definitions is shown in **Figure 1**.

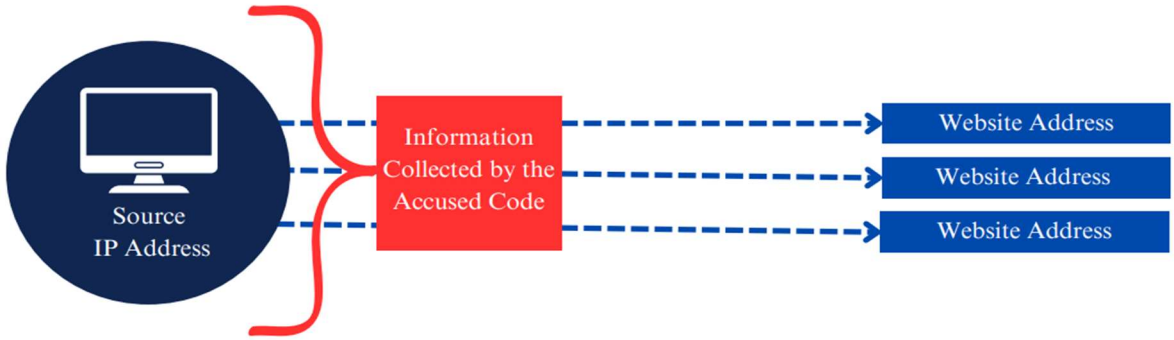
Figure 1.



Here, the Accused Code is not a pen register because it does not operate as shown in Figure 1, and Plaintiffs do not argue otherwise. Even if collecting an IP address were equivalent to collecting a phone number, which it is not, Plaintiffs do not allege that the Accused Code collects any *recipient* "dialing, routing, addressing, or signaling information" relating to an outgoing communication. *See, e.g., U.S. v. Soybel*, 13 F.4th 584, 589 (7th Cir. 2021) ("the pen register associated with his apartment recorded connections between his private IP address and the IP addresses of those websites that internet users in the apartment had visited. The pen registers revealed that Soybel's private IP address—and only Soybel's private IP address—attempted to connect to KeepStock 790 times"). Rather, Plaintiffs here only allege that the Accused Code collected the IP address of *their own computers (the originating or source IP address)* and not

the IP address of any website visited by plaintiff or the IP address of any other device with whom Plaintiffs communicated. *See, e.g.,* Dkt. 15 ¶¶ 90, 91, 97, 102. This accused process, as shown in **Figure 2** below, is not how a pen register operates.

Figure 2.



This fundamental disconnect between the operation of the Accused Code and a pen register is confirmed by examining other sections of the California pen register rule, which render Plaintiffs' theory of liability nonsensical when applied to the Accused Code. For one example, Section 638.52 provides the procedure for a law enforcement officer to apply and gain authorization to use a pen register. Cal. Penal Code § 638.52. This section provides that the court order authorizing pen register use must include the "number …of the telephone line to which the pen register …is to be attached" and "[t]he identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register…is to be attached." Cal. Penal Code § 638.52(d)(1), (d)(3). This means, even to apply for a court order allowing for the installation of a pen register, law enforcement officials *must already have* the source phone number of the individual to be tracked by the pen register. And again assuming that phone numbers and IP addresses are equivalent (which they are not), it would be nonsensical to apply for authorization to install the Accused Code as a pen register, because just to apply for such permission, law enforcement would need to have the only piece of information that the Accused Code is capable of collecting – the source identifier (IP address) of the user's device. CIPA's "trap and trace" definition provides another differentiating example. Section 638.50(c) defines a "trap and trace" device as "a device or process that captures the *incoming* electronic or other

impulses that identify the *originating number* or other dialing, routing, addressing, or signaling information reasonably likely to identify the *source* of a wire or electronic communication…[.]" (emphasis added). This device is thus the flip side of a pen register—it is used to find the source of a communication, where the pen register is used to gather information to identify its recipient. The "pen register" definition does not mention the "originating number" and "source" of a communication, but instead focuses on the routing information for the "transmission" of a communication. Section 638.50(b). This also shows why the Accused Code, which only allegedly collects "originating" "source" information, is not a pen register. Plaintiffs do not claim the Accused Code is a trap and trace device. Dkt. 15 ¶ 117.

It is also telling that federal courts, applying the federal pen register statute that inspired the CIPA law, have rejected attempts to classify technology used to discover an individual's source phone number as a pen register. For example, a federal court in Texas found that "equipment designed to capture… cell phone numbers" within a geographic area, which the government meant to use to weed out and discover the phone number of a target individual, was not a pen register under the federal pen register statute. *In re the Application of the U.S. for an Ord. Authorizing the Installation & Use of a Pen Reg. & Trap & Trace Device*, 890 F. Supp. 2d 747, 748, 750-52 (S.D. Tex. 2012). Because the government did not already have the phone number of the individual to be tracked, and therefore "the plain language of the statute [that] mandate[d] that th[e] Court have a telephone number or some similar identifier before issuing an order authorizing a pen register" could not be met, the court held that the government had "not provided any support that the pen register statute applies to" the technology it proposed to install, and that the "pen register [statute] d[id] not apply to this type of electronic surveillance." *Id.* at 751-52. Likewise, here, because the Accused Code is only meant to collect the user's source IP address, which information would already have to be known for a court to authorize installation of such code, the pen register statute cannot apply.

ii. The Accused Code Is Not a Pen Register If It Collects Communications

The Accused Code is also not a pen register because – at least as alleged in Plaintiffs' FAC – it appears to collect "the contents of a communication." Cal. Penal Code § 638.50(b).

Specifically, Plaintiffs claim repeatedly that the IP address collected by the Accused Code is either contained within a transmitted cookie or sent as a "standalone" transmission. Either way, this does not match the pen register definition. Section 630.50(b) defines "pen register" as a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Broken-down, this definition differentiates between two types of information relating to the transmission of a communication: the "dialing, routing, addressing, or signaling information" of a communication and 2) "the contents of a communication." A pen register collects the former but not the latter. As described in the prior section, the Accused Code is not a pen register because the source IP addresses it allegedly collects are not "dialing, routing, addressing, or signaling information." But the Accused Code is also not a pen register for the separate reason that, as alleged in the FAC, it may collect something more akin to the "the contents of a communication."

As a threshold matter, it is hard to parse what Plaintiffs believe the "communications" might be, because Plaintiffs fail to identify any. Nowhere in the FAC do Plaintiffs identify any "communication" whose "dialing, routing, addressing, or signaling information" was allegedly collected by the Accused Code as required by Cal. Penal Code § 638.50(b). This is a telling omission, given that the pen register definition hinges on the type of information that the accused device or process may or may not gather from a transmitted communication: if a technology collects "dialing, routing, addressing, or signaling information," it might be a pen register, but if it collects the "communication" itself, it is not. *See* § 638.50(b); *Capitol Recs. Inc*., 2009 WL 1664468, at *3 (finding that the federal pen register act "ha[d] no application…because the IP address recorded by MediaSentry was part of the content of the communication."). Consequently, Plaintiffs' failure to specifically identify any communication whose "dialing, routing, addressing, or signaling information" is supposedly recorded by the Accused Code is an omission that makes Plaintiffs' claim incomprehensible. Although Fandom highlighted this issue in its prior motion to dismiss, Dkt. 11 at 9-11, Plaintiffs still do not specifically identify any relevant "communications" in the FAC. *See* Dkt. 15-1.

Although Plaintiffs cursorily allege that the Accused Code "do[es] not collect the content of Plaintiffs' and the Class's electronic communications with the Website," Dkt. 15 ¶ 119, the Court need not accept this conclusory statement. *See Iqbal*, 556 U.S. at 678 ("a formulaic recitation of the elements of a cause of action will not do"). Especially when, as here, it is contradicted by other allegations in the FAC. For example, Plaintiffs state multiple times in the FAC that their IP addresses are collected and sent by the Accused Code "through" or "within" a transmitted cookie – that is, sent as the *content* of communications. *See e.g.,* Dkt. 15 ¶ 37, (Accused Code "instructs the user's browser to send the user's IP address *through* the cookie"), ¶ 48 ("Audiencerate will continue to receive the user's IP address *through* the cookie"), ¶ 91 (Plaintiff Shah's IP address allegedly sent both "as standalone data" and "*within* [a] cookie") (all emphases added). The FAC's figures confirm this, literally showing IP addresses located inside allegedly transmitted cookies. *See, e.g., id.*, Figures 5-6, 10-11 (highlighting IP addresses located within "cookie" fields). But as caselaw under the federal pen register statute shows, if the Accused Code obtains IP addresses in this manner as Plaintiffs allege, as the content of a communication, it is not a pen register. *See e.g., Malibu*, 2013 WL 12180709, at *4 ("In the instant case, the IP address received by IPP was part of the content of the communication, so the Pen Register Act has no application"); *Capitol Recs. Inc,* No. 2009 WL 1664468, at *3 ("The Pen Register Act has no application here because the IP address recorded by MediaSentry was part of the content of the communication.").

Thus, to the extent the FAC suggests that the Accused Code obtains Plaintiffs' IP addresses as the contents of a communication between Plaintiffs' browsers and third-party servers, the Accused Code is not a pen register, and the FAC should be dismissed.

C. The Accused Code Is Not A "Pen Register" Because It Is Not Used in Conjunction With Telephonic Technology

Plaintiffs' claim also fails because the text and legislative history of Section 638.51 and related provisions make clear that the statute applies only to "device[s] or process[es]" used for *telephone* surveillance and tracking. It does not apply to software that collects the source IP address from a user's computer, as the Accused Software is alleged to do here.

As described above, a "pen register" was traditionally a "mechanical device which records the numbers dialed *from a telephone*," without overhearing the oral communications. *People v. Blair*, 25 Cal. 3d 640, 654 n.11 (1979) (emphasis added); *Smith*, 442 U.S. at 736 n.1 (1979) (a pen register "records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released"). This purpose of enabling telephone line tracking is mirrored throughout the legislative history of CIPA's pen register sections and reflected in their legislative text. For example, the April 29, 2015 analysis of the California assembly bill that proposed the pen register sections stated its purpose as authorizing "state and local law enforcement agencies to seek an emergency order to use pen registers and trap and trace devices in *telephone surveillance.*" *See* Jones Decl., Ex 11 at 1 (California Bill Analysis, A.B. 929 Assem., April 21, 2015) (emphases added). The author of the bill was later quoted in the legislative record as stating that the purpose of the law was to authorize law enforcement use of "a 'pen register' which allows law enforcement officers to record all *outgoing numbers from a particular telephone line*." *See* Jones Decl., Ex 13 at 3 (Concurrence in Senate Amendments, AB 929, June 17, 2015) (emphasis added).

Likewise, the text of multiple sections of the California law confirm that the term "pen register" is limited to devices and applications operating in a telephonic context. For example, the section immediately following Section 638.51 provides that a pen register may not collect the physical location of the subscriber "except to the extent that the location may be determined *from the telephone number*" to be tracked. Cal. Penal Code § 638.52(d) mandates that any court order authorizing law enforcement to use a pen register must include the "[t]he number and, if known, physical location of the *telephone line* to which the pen register or trap and trace device is to be attached."

Based on such considerations, a California court recently found that the language of Section 638.50 and CIPA generally limits the statute to applications that involve "telephonic functionality." *Licea*, Minute Order at 4-5 (dismissing Section 638.51 claim based on website technology). Specifically, the court found that the complaint's general allegations of a "'device' without any actual specific reference to a mobile phone or other potential form of communication device potentially qualifying as a cellular device," indicated that the claim lacked factual support.

Id. at 6. The same result should follow here, where Plaintiffs do not claim that the Accused Code performed any sort of telephonic surveillance or has any telephonic functionality. Rather, both Plaintiffs expressly concede that they only attempted to connect to Fandom's website using desktop computers. Dkt. 15 ¶¶ 89, 96. Based on these allegations alone, Plaintiffs' claim fails because they do not show that Accused Code is a device or process associated in any way with telephonic surveillance.

Plaintiffs may nevertheless attempt to argue the Accused Code "is at least a 'process'" under California Penal Code § 638 because it is "software that identifies consumers, gathers data, and correlates that data," parroting language from *Greenley v. Kochava*. 2023 WL 4833466, at **15. But this out-of-district case does not apply to the facts here. To begin, *Greenley* involved software on a mobile phone, something that is not alleged here. *Compare id.* at **15 ("surreptitiously embedded software installed in a *telephone*") with Dkt. 15 ¶¶ 89, 96 (Plaintiffs accessed Fandom website from desktop computers). Further, *Greenley* involved a complex software that collected a multitude of user data, including "geolocation," "search terms, click choices, purchase decisions and/or payment methods," and used that to "fingerprint" "each unique device and user." *Id*. at **1, **15. Arguably, such a vast collection of data from a user's cellular telephone (which included the user's precise real-time location, information on places the user went with the mobile phone in hand, and surely included information on the websites the user visited to "click choices" or "purchase" items) might be viewed as having some hallmarks in common with the species of "telephone surveillance" that Section 638.51 means to prevent. However, there is no analog between *Greenley* and the situation here, where Plaintiffs only allege the collection of the IP addresses of their stationary desktop computers, and nothing more. Plaintiffs do not allege the Accused Code collected any other type of information, and so any claim that Fandom could or does use the collected IP address to generate "unique 'fingerprinting'" for website users is pure speculation. *See id.* at **15.

Because Plaintiffs do not allege that the Accused Code has any connection to telephone technology or functionality and allege no behavior that bears any conceivable comparison to telephone surveillance, Plaintiffs' FAC should be dismissed.

D. Plaintiffs Do Not Plausibly Allege that Fandom "Installed" or "Used" the Accused Code

The FAC should also be dismissed for the separate reason that Plaintiffs fail to plausibly allege that Fandom "install[ed] or use[d]" the alleged pen register under Section 638.51(a).

Plaintiffs' allegations that Fandom installed and used the Accused Code on their browsers may be disregarded, as they do not allege facts that plausibly support that conclusory allegation. *See, e.g.* Dkt. 15 ¶¶ 23, 66, 67, 90, 97; *Iqbal*, 556 U.S. at 678 (2009) ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."). Instead, the FAC focuses on the actions of third parties GumGum, Audiencerate, and TripleLift, whom Plaintiffs concede develop, install and use the Accused Code. *See, e.g.,* Dkt. 15, ¶¶ 33, 42, 52. For example, the FAC stresses that the data allegedly collected by the Accused Code was sent directly to and then used by GumGum, Audiencerate, and TripleLift. *See, e.g.*, Dkt. 15 ¶ 62, ¶ 78 ("GumGum collects users' IP addresses through its GumGum Tracker"); ¶ 82 ("This is why Audiencerate collects IP addresses: it allows Audiencerate to segment users in order to run targeted campaigns and perform data analysis"); ¶ 88 ("TripleLift collects users' IP addresses through its TripleLift Tracker"). Indeed, the FAC identifies the Accused Code as belonging to these third parties. *See* Dkt. 15 ¶ 35 ("GumGum uses *its* Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website"); *id*. ¶ 45 ("Audiencerate uses *its* Tracker to receive, store, and analyze data sent collected from website visitors, including visitors of Defendant's Website."); *id*. ¶ 54 ("TripleLift uses *its* Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.") (all emphasis in the foregoing added). Yet the FAC does not claim that the Accused Code sends any information directly to Fandom, and says nothing about how the IP addresses collected by third parties allegedly end up in Fandom's hands. The FAC also never addresses the fundamental question why Fandom would install or use the Accused Code, when Fandom already receives IP address information every time a user voluntarily provides their IP addresses to Fandom's web servers in visiting the website. Plaintiffs thus fail to plead sufficient facts to nudge the FAC from Fandom *possibly* installing or using the Accused Code, to *plausibly*

doing so. *See e.g., Esparza v. Lenox Corp*., No. C 22-09004 WHA, 2023 WL 2541352, at *3 (N.D. Cal. Mar. 16, 2023) (finding that "[w]ithout further elaboration, plaintiff's allegations that someone eavesdropped and intercepted chat messages [were] merely conclusory recitations of the CIPA wiretapping statute, and not entitled to the presumption of truth" and consequently, "Plaintiff's claim of a CIPA violation [wa]s therefore insufficient to withstand dismissal."). Accordingly, Plaintiffs' claims fail for this reason too.

E. The FAC Should Be Dismissed with Prejudice

Plaintiffs' First Amended Complaint confirms they cannot state a claim against Fandom: it merely restates the same claims already presented once before and shows that no amendment can overcome the deficiencies of Plaintiffs' claims. The Court may dismiss a case with prejudice when amendment would be futile. *See Ascon Prop., Inc. v. Mobil Oil Co*., 866 F.2d 1149, 1160 (9th Cir. 1989) ("Leave need not be granted where the amendment . . . constitutes an exercise in futility[.]"). This is such a case. Plaintiffs' claims are futile because they cannot plausibly allege violations of California's pen register law. Plaintiffs can allege no facts to plausibly suggest that the Accused Code meets the definition of "pen register" under California law. Because Plaintiffs cannot cure these fundamental defects, the Court can and should dismiss the First Amended Complaint without leave to amend.

VI. CONCLUSION

For these reasons, the Court should grant the Motion and dismiss Plaintiffs' FAC without leave to amend. Plaintiffs' attempt to characterize a piece of code that captures a user's voluntarily provided IP address (and nothing more) as a pen register stretches the language and meaning of California criminal laws beyond recognition and ignores the extensive caselaw holding otherwise. Plaintiffs' misguided interpretation of California law would expose all website operators to criminal liability and statutory damages in California, based merely on the basic or normal functioning of their websites, which cannot be the intent of CIPA. Plaintiffs' amended claims should be dismissed with prejudice.

///

Respectfully submitted,
TYZ LAW GROUP PC

Dated: May 30, 2024

/s/Erin Jones
Erin Jones

Attorneys for Defendant
FANDOM, INC.